

University of Connecticut VoTeR Center



Voting Technology Research Center

*Informational Presentation
to Government Administration and Elections Committee*

Monday, March 10, 2008

PI: Alexander Shvartsman
Co-PIs: Aggelos Kiayias
Laurent Michel
Alexander Russell

{aas,aggelos,ldm,acr}@cse.uconn.edu



Some “Pre-history”

- Year 2000 elections and aftermath
- Rush to “computerized” voting systems
 - ❑ Better accessibility and precision – good reasons!
 - ❑ “Bleeding” edge adoption
- Issues with technology
 - ❑ Premature deployment of immature technology
 - ❑ Potential for reducing errors and controlling interference
 - ❑ Potential for increasing errors and allowing interference
- Deployment of new technology
 - ❑ Must be methodical, careful, diligent
 - ❑ Acknowledging limitations and risks



VoTeR Center: Background

- Participation in the CT VTSB, 2005-2006
- Participation in the 2006 CFP
- Relationship with the CT SOTS Office since 2006
 - ❑ Formal agreement is in place; funding 2006-2008
 - ❑ Advising on the voting technology issues
 - ❑ Evaluation of proposed voting equipment
 - ❑ Design and implementation of tests of technology
 - ❑ Participation in pre-/post- election audits
 - ❑ Recommendation on safe use procedures
 - ❑ Publication of findings (see <http://voter.engr.uconn.edu>)



VoTeR Center Staff

- A. Shvartsman, PI
 - Dependable Systems, Fault-Tolerance, NSF Career Award
- A. Kiayias, Co-PI
 - Cryptography, Voting Systems, NSF Career Award
- L. Michel, Co-PI
 - Software Systems, Constraints Prog., NSF Career Award
- A. Russell, Co-PI
 - Cryptoraphy, Security Guarantees, NSF Career Award
- Graduate Assistants:
 - S. Davtian, S. Kentros, K. Konwar, N. Nicolaou, A. See, K. Shashidhar, other graduate and undergraduate students



VoTeR Center Capabilities

- Voting technology expertise
- Dependability and fault-tolerance
- Security and cryptography
- End-to-end security analysis
- Black-box analysis
- Reverse engineering of voting equipment
- Design of software for security evaluation
- Pre-election and post-election testing
- Audits



Voting Equipment Evaluation

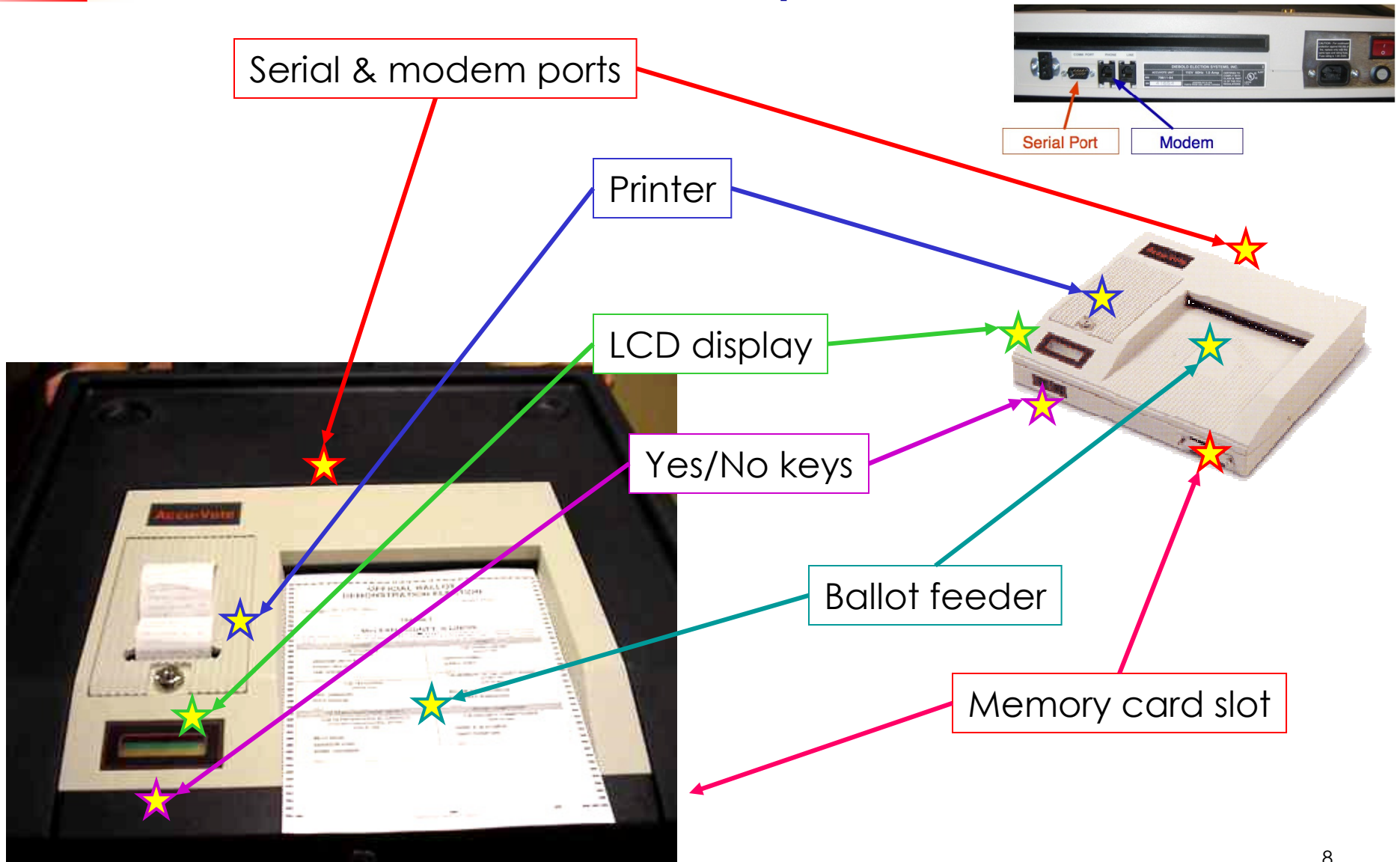
- Activity since Spring 2006
- VoTeR Center evaluated several systems
 - ❑ AccuVote Optical Scan system
 - ❑ IVS Inspire vote-by-phone system
 - ❑ Others
- The evaluations are done in the UConn VoTeR Lab
 - ❑ Black-box evaluation and reverse engineering
 - ❑ Exploration of possible attack vectors
 - ❑ Physical integrity
 - ❑ Mitigation strategies and safe use recommendations

AccuVote Optical Scan

- Manufactured by Premier (Diebold)
- Provided in CT by LHS Associates
- Assessed by VoTeR Lab at UConn
 - ❑ Inherently provides voter-verified paper trail, enabling audits, and manual and machine recounts
 - ❑ In the absence of strict chain of physical custody procedures is a potential target of several attack vectors (developed by ourselves and other workers)
 - ❑ Reports: <http://voter.engr.uconn.edu>



AccuVote Optical Scan





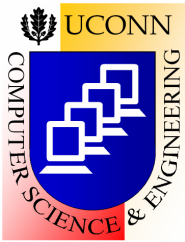
AccuVote and GEMS

- AccuVote Optical Scan tabulator
 - ❑ Firmware version 1.96.6 (EPROM)
 - ❑ V25 CPU, 8088 compatible
 - ❑ Epson 40-pin 128KB memory card
- GEMS Election Management System
 - ❑ Ballot layout: bubble geometry and counters
 - ❑ Bytecode: program to be loaded into memory card
- Memory cards
 - ❑ Inserted into AccuVote OS
 - ❑ Loaded from GEMS via serial line



Accomplishments & Current Focus

- Security analysis of AccuVote Optical Scan
- Threat vector assessment and design
- Safe use procedure recommendation
- Assistance with audit design and analysis
- Complete analysis of memory cards
- Reverse-engineering of firmware and protocols
- Assessment of software/firmware upgrades
- Precision analysis
- Technology / issue tracking



November 2007 Elections

- Test of Memory cards
 - ❑ Integrity of ballot layout and counters vs. GEMS data
 - ❑ Byte correct safety: counting and printing, no other code
- Pre-election testing of memory cards
 - ❑ 522 cards analyzed
 - ❑ http://voter.engr.uconn.edu/voter/Reports_files/Audit07-h-080130.pdf
- Post-election testing of memory cards
 - ❑ 100 cards analyzed
 - ❑ http://voter.engr.uconn.edu/voter/Reports_files/audit07mc-post.pdf
- Statistical analysis of audit returns
 - ❑ http://voter.engr.uconn.edu/voter/Reports_files/Audit07-h-080130.pdf

Pre-election Card Test

	For cards received before election		For cards received after election	
	Number	% Total	Number	% Total
(a) Card Format				
Good Data, Clean Card	362	96.2%	495	94.8%
Good Data, Some "Specks"	6	1.1%	9	1.7%
Junk Data	10	2.6%	18	3.4%
Totals:	378	100%	522	100%
(b) Card Status				
Not Programmed (Blank)	0	0.0%	0	0.0%
Not Set for Election	167	45.4%	218	43.3%
Set for Election	181	49.2%	233	46.2%
Results Print Aborted	7	1.9%	11	2.2%
Election Closed	13	3.5%	42	8.3%
Results Sent/Uploaded	0	0.0%	0	0.0%
Audit Report Printed	0	0.0%	0	0.0%
Totals:	368	100%	504	100%
(c) Counter Status				
Zero Counters	209	56.8%	285	56.5%
Non Zero Counters	158	42.9%	218	43.3%
Non Zero and Set for Election	1	0.3%	1	0.2%
Totals:	368	100%	504	100%
(d) Election Count: (Number of test elections)				
1	361	98.1%	485	96.2%
2	6	1.6%	16	3.2%
3	0	0.0%	2	0.4%
4	1	0.3%	1	0.2%
Totals:	368	100%	504	100%



Post-election Card Test

	Number of Cards	% Total Cards
(a) Card Format (all cards)		
Good Data, Clean Card	92	92.0%
Good Data, Some "Specks"	0	0.0%
Junk Data	8	8.0%
Total:	100	100%
(b) Card Status (well-formatted cards)		
Not Programmed (Blank)	1	1.1%
Not Set for Election	11	12.0%
Set for Election	44	47.8%
Results Print Aborted	4	4.3%
Election Closed	32	34.8%
Results Sent/Uploaded	0	0.0%
Audit Report Printed	0	0.0%
Totals:	92	100%
(c) Counter Status (usable cards)		
Not Set for Election, Non Zero Counters	11	12.1%
Set for Election, Zero Counters	43	47.3%
Set for Election, Non Zero Counters	1	1.1%
Election Closed, Non Zero Counters	32	35.2%
Print Aborted, Non Zero Counters	4	4.4%
Totals:	91	100%
Total number of cards used in the election:	36	39.6%



Audit Analysis Highlights

- 958 records received
 - ❑ 783 records (about 70%) complete, and contained no obvious errors
 - ❑ 175 records (18.3%) incomplete, unusable, or incorrect
 - ❑ 111 records (11.6%) usable, but incomplete data, or arithmetic errors
- 783 records that are sufficiently complete to perform the analysis
 - ❑ 520 records (66.4%) show discrepancy of 0 or 1 votes
 - ❑ 700 records (89.4%) show discrepancy of 5 votes or lower
 - ❑ 31 records (4.0%) show discrepancy of 10 or more votes
 - ❑ Adjusting for undercounts due to questionable ballots yielded 716 records (91.4%) showing discrepancy of 5 votes or lower
 - ❑ The largest errors are due to errors in audit reporting
- Average discrepancy is 0.9 votes per race, where the average count consisted of 277 votes
- *Lesson: Revise audit definition and instructions (in progress)*



Current and Planned Work

- Post-election memory card audit for 2008 primaries
- Preparation for November 2008
 - Improve memory card audits
 - Assist with definition of hand-counted audits
 - Refinement of safe use procedures
- New techniques to improve security/integrity
 - Design experiments to assess optical scan precision
 - Design means for automated printed ballot analysis vs. memory cards
 - Tools for audits and alternate counting in audits
- Firmware evaluation
 - Upgrades to next versions: evaluation and recommendation
 - Firmware safety analysis
- Respond to State needs



Summary

- VoTeR Center
 - ❑ Providing voting technology expertise to Connecticut
- Current work is focused on AccuVote Optical Scan
 - ❑ Assessment of precision and vulnerabilities
 - ❑ Safe use procedures & strict chain of physical custody
 - ❑ Memory card integrity testing and post-election audits
 - ❑ Upgrades; technology tracking & issues
- Futures and plans:
 - ❑ Technological means of strengthening integrity, end-to-end
 - ❑ Voting technology: research & development